UNITED STATES DISTRICT COURT FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	:	
	:	Case No. 17-cr-00684-ER
v.	:	
	:	ECF Case
LAMONT EVANS EMANUEL RICHARDSON, a/k/a "Book," ANTHONY BLAND, a/k/a "Tony," CHRISTIAN DAWKINS, and MERL CODE,	:	
Defendants.	:	

DEFENDANTS' MEMORANDUM OF LAW IN SUPPORT OF THEIR JOINT MOTION TO SUPPRESS EVIDENCE OBTAINED FROM THE SEARCH OF DEFENDANTS' CELL PHONES

NEXSEN PRUET LLC
William W. Wilkins
Mark C. Moore
Andrew A. Mathias
55 E. Camperdown Way, Suite 400
Greenville, South Carolina 29601
(864) 370-2211
Attorneys for Defendant Merl Code

HANEY LAW GROUP PLLC
Steven A. Haney
3000 Town Center Drive, Suite 2570
Southfield, Michigan 48075
(248) 414-1470
Attorneys for Defendant Christian Dawkins

BARNES AND THORNBURG, LLP
William R. Martin
1717 Pennsylvania Ave
Suite 500
Washington, DC 20006
(202) 465-8422
Attorneys for Defendant Lamont Evans

LAW OFFICES OF JEFFREY LICHTMAN
Jeffrey B. Einhorn
Jeffrey Lichtman
11 E. 44th Street, Ste. 501
New York, New York 10017
(212) 581-1001
Attorneys for Defendant Anthony "Tony" Bland

MORDOCK BARBER, LLC
Craig J. Mordock
7611 Maple Street, Suite A3
New Orleans, Louisiana 70118
(504) 304-2335
Attorneys for Defendant Emanuel "Book" Richardson

TABLE OF CONTENTS

TABLE OF AUTHORITIES

Cases

Other Authorities

Rules

Defendants Christian Dawkins and Merl Code (collectively "Defendants")[1] respectfully submit this memorandum of law in support of their motion to suppress all evidence seized pursuant to the search of their cell phones.

PRELIMINARY STATEMENT

One of the most intrusive of all investigative methods is the unfettered search of a modern cell phone, through which law enforcement can access the most intimate details of an individual's life. Cell phones are much more than devices used to make telephone calls. Indeed, they are portable computers, capable of storing an ever-increasing amount of deeply personal data, which chronicle every aspect of a person's existence. Cell phones track every website that the owner has visited. They record exactly where the owner was on a particular day, and for exactly how long. They store intimate photographs and videos that the owner has taken. They contain a record of the owner's private communications. In short, a cell phone is a window into its owner's entire life. For this reason, the Fourth Amendment demands scrupulous adherence to strict requirements before the government may search the entire contents of an individual's cell phone. The government failed to comply with those requirements here.

Based on evidence that Mr. Code used his phone for thirteen calls, and evidence that Mr. Dawkins used his phone for twenty calls and a single text message, the Government obtained warrants to search the entirety of the data contained on Defendants' cell phones—including photographs, videos, internet search history, applications, emails, calendars, and other matter. The fact that the phones were used for calls, however, does not create probable cause to believe

[1] The cell phones of Defendants Lamont Evans and Anthony Bland a/k/a "Tony" were neither seized nor searched by law enforcement. In addition, Defendant Emanuel Richardson a/k/a "Book" voluntarily surrendered his cell phone to the Federal Bureau of Investigation. As such, no warrants exist to seize and search the cell phones of Mr. Evans, Mr. Bland, or Mr. Richardson.

that evidence of criminality would be found within the electronic data contained on the phones. It goes without saying that the content of phone calls does not reside on the phones used to make those calls. But other than these calls, and, with respect to Mr. Dawkins, a single text message, the Government's search warrant applications presented no evidence that the ***data*** on Defendants' phones contained incriminating evidence. The few communications identified in the warrant applications do not provide probable cause to believe evidence of a crime may be found on Defendants' phones—and do not support the all-encompassing sweep of electronic data contained therein that the warrants authorized. The Fourth Amendment does not permit this sort of "general, exploratory rummaging in a person's belongings." Accordingly, any evidence seized from the searches of Defendants' cell phones should be suppressed, and the Government should immediately return Defendants' cell phones, as well as the imaged copies of the cell phone data it maintains, to Defendants.

FACTUAL BACKGROUND

Following Defendants' arrests, the Government submitted applications for warrants to search their cell phones (the "Warrant Applications" or "Applications"). (*See* Ex. 1 (Code Application); Ex. 2 (Dawkins Application).) The warrants were issued on the same day the Applications were submitted (the "Search Warrants" or "Warrants"). (*See* Ex. 3 (Code Warrant); Ex. 4 (Dawkins Warrant).)

A. The Government's Warrant Applications.

Each of the Warrant Applications described evidence of the scheme alleged in the Complaint and Indictment, but provided virtually no connection between this alleged misconduct and the electronic data stored on Defendants' phones. With respect to Mr. Code, the Government's Application purports to establish probable cause sufficient to seize and search his

cell phone based on evidence of thirteen phone calls—recorded over a span of three months—in which Mr. Code participated via his BlackBerry Passport phone. (Ex. 1 at MC_00000011-17.) The content of these calls, of course, would not reside on Mr. Code's phone. The Application also states that during one of these calls, Mr. Dawkins informed Mr. Code that he would text Mr. Code a list of coaches Mr. Code could introduce to UC-1. (*Id*. at MC_00000014, ¶17(b).) With respect to Mr. Code's Kyocera phone, the Application identifies one intercepted call in which Mr. Code and Mr. Dawkins purportedly discussed payments in furtherance of the charged offenses, and notes that Mr. Code was in possession of the Kyocera phone when he was arrested. (*Id*. at MC_00000016, ¶20.)

As to Mr. Dawkins, the Warrant Application cites a total of twenty calls and one text message, intercepted over a period of four months, tied to Mr. Dawkins's black iPhone. (Ex. 2 at CD_00000083-84.) With respect to Mr. Dawkins's white iPhone, the Application references an intercepted call between Mr. Dawkins and Mr. Code "[redacted]," and notes that Mr. Dawkins was carrying the white iPhone on his way to a meeting with an undercover agent when he was arrested. (*Id.* at CD_00000084 ¶18.)

Beyond references to the use of these phones for calls (one of which indicated Mr. Dawkins would text Mr. Code) and a single intercepted text message, the Warrant Applications provide no basis to conclude that evidence of criminality would be found in the emails, internet search history, notes, photos, videos, or in any of the other data contained on Defendants' phones. To fill that void, the authoring FBI agent asserts in the Application with respect to Mr. Code that, based on his "[redacted]," he "[redacted]

[redacted]

[redacted]" Ex. 1 at MC_00000016, ¶1, 21.) The Dawkins Application offers the more limited—but entirely generic—observation that cell phones "[redacted]." (Ex. 2 at CD_00000081, ¶6.)

B. The Authorizations in the Warrants.

The Code Warrant authorizes the search of Mr. Code's cell phones for, among other things, "[redacted]" to a multitude of individuals and entities. (Ex. 3 at MC_00000114, Item II(c).) Among other things, the Dawkins Warrant authorizes the search of Mr. Dawkins' cell phones for "[redacted]" (Ex. 4 at CD_00000183, Item II(c).)

Despite the limited detail provided by the Warrant Applications, the Search Warrants broadly and generally authorized law enforcement to search the *entirety* of the data contained on Defendants' phones:

[redacted]

(Ex. 3 at MC_00000115; Ex. 4 at CD_00000184.) (emphasis added).) The Warrants further state that "[redacted]

[redacted]." (*Id*. (emphasis added).)

STANDARD OF REVIEW

The Fourth Amendment mandates that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or affirmation, and particularly describing the place to be searched, and the persons or things to be seized." U.S. Const. amend. IV. The "specific evil" that the Fourth Amendment aims to combat "is the 'general warrant' abhorred by the colonists[.]" *Coolidge v. New Hampshire*, 403 U.S. 443, 467, 91 S. Ct. 2022, 2038 (1971). To that end, the Fourth Amendment protects against "wide-ranging exploratory searches" unsupported by probable cause. *Maryland v. Garrison*, 480 U.S. 79, 84, 107 S. Ct. 1013, 1016 (1987).

Given the nature and concentration of deeply personal information that people store on computers, cell phones, and other forms of electronic devices, the Second Circuit has recognized that the Fourth Amendment's privacy protections are particularly important in connection with the searches of electronic data. The Second Circuit has explained that "advances in technology and the centrality of computers in the lives of average people have rendered the computer hard drive akin to a residence in terms of the scope and quantity of private information it may contain," and that "[t]here is, thus, a serious risk that every warrant for electronic information will become, in effect, a general warrant, rendering the Fourth Amendment irrelevant." *United States v. Galpin*, 720 F.3d 436, 446-47 (2d Cir. 2013) (quoting *United States v. Comprehensive Drug Testing, Inc.*, 621 F.3d 1162, 1176 (9th Cir. 2010) (quotation marks omitted)); *see also United States v. Ganias*, 755 F.3d 125, 134-35 (2d Cir. 2014) *rev'd en banc on other grounds*, 824 F.3d 199 (2d Cir. 2016)

("The[] Fourth Amendment protections apply to modern computer files. Like 18th Century 'papers,' computer files may contain intimate details regarding an individual's thoughts, beliefs, and lifestyle, and they should be similarly guarded against unwarranted Government intrusion. If anything, even greater protection is warranted.").

The Supreme Court shares the Second Circuit's concerns. It has emphasized the potential for privacy invasion inherent in searches of cell phones. In particular, the Court has noted that "a cell phone collects in one place many distinct types of information—an address, a note, a prescription, a bank statement, a video—that reveal much more in combination than any isolated record," and that "[t]he sum of an individual's private life can be reconstructed through a thousand photographs labeled with dates, locations, and descriptions[.]" *Riley v. California*, 134 S. Ct. 2473, 2489 (2014). For this reason, a digital search "demands a heightened sensitivity" to the requirements of the Fourth Amendment. *Galpin*, 720 F.3d at 447.

"[A] warrant may not be issued unless probable cause is properly established and the scope of the authorized search is set out with particularity." *Kentucky v. King*, 563 U.S. 452, 459, 131 S. Ct. 1849, 1856 (2011). In addition to ensuring that there is probable cause to seize and search a cell phone, courts must also give special attention to whether a warrant to search a cell phone is impermissibly overbroad. A search warrant is overbroad in violation of the Fourth Amendment if its "description of the objects to be seized is . . . broader than can be justified by the probable cause upon which the warrant is based." *Galpin*, 720 F.3d at 446; *see also United States v. Hernandez*, No. 09CR625(HB), 2010 WL 26544, at *8 (S.D.N.Y. Jan. 6, 2010) (courts must focus on whether probable cause exists "to support the breadth of the search that was authorized.") (*quoting United States v. Dinero Express, Inc.,* 99-CR-975, 2000 WL 254012, at *9 (S.D.N.Y. Mar. 6, 2010) (quotation marks omitted)); *see also United States v. Cioffi*, 668 F. Supp.

2d 385, 390 (E.D.N.Y. 2009) ("Breadth deals with the requirement that the scope of the warrant be limited to the probable cause on which the warrant is based.") (quoting *United States v. Hill*, 459 F.3d 966, 973 (9th Cir. 2006) (quotation marks omitted)). A warrant that purports to "authorize the seizure of, essentially, all documents" from a property exceeds the scope of probable cause. *United States v. Wey*, 256 F. Supp. 3d 355, 393 (S.D.N.Y. 2017).

In the context of searches of electronic data, the Government is permitted to "mirror" or copy the data to execute the search. *United States v. Ganias*, 824 F.3d 199, 215 (2d Cir. 2016); *see also* Fed. R. Crim. Pro. 41(e)(2)(B) (a warrant "may authorize the seizure of electronic storage media or the seizure or copying of electronically stored information" and may "authorize[] a later review of the media or information consistent with the warrant."). But the scope of the search of any copied or imaged data must be limited by the probable cause underlying the search warrant. *Galpin*, 720 F.3d at 453 (suppressing evidence obtained from an electronic search when the search went "beyond the scope" of the probable cause).

Evidence obtained in violation of the Fourth Amendment must be excluded. *Herring v. United States*, 555 U.S. 135, 139, 129 S. Ct. 695, 699 (2009). Suppression is the appropriate remedy where the affidavit submitted in support of a search warrant is "'so lacking in indicia of probable cause as to render official belief in its existence entirely unreasonable.'" *United States v. Leon*, 468 U.S. 897, 923, 104 S. Ct. 3405, 3421 (1984) (*quoting Brown v. Illinois*, 422 U.S. 590, 609, 95 S. Ct. 2265 (1984)). Additionally, "a warrant may be so facially deficient—*i.e.*, in failing to particularize the place to be searched or the things to be seized—that the executing officers cannot reasonably presume it to be valid," and evidence obtained from a search pursuant to such a warrant must be suppressed. *Leon*, 468 U.S. at 923. 104 S. Ct. at 3421 (1984); *see also United States v. Rosa*, 634 F.3d 639, 641 (2d Cir. 2011) (Kaplan, J., dissenting) ("exclusion is appropriate where, as here, a reasonable officer could not have

presumed the warrant to have been valid."). "The burden is on the government to demonstrate the objective reasonableness of the officers' good faith reliance" on an invalidated warrant. *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992).

ARGUMENT

A. The Warrants do not Establish Probable Cause to Seize and Search Defendants' Cell Phones.

A search warrant application purporting to establish that an individual has engaged in criminal activity does not provide probable cause to search the entirety of that individual's possessions. *See United States v. Pabon*, 871 F.3d 164, 181 (2d Cir. 2017) ("[A] determination of probable cause to search is not the same as a determination that there is, at the same time, probable cause to arrest, or vice versa."); *United States v. Burton*, 288 F.3d 91, 103 (3d Cir. 2002) ("[P]robable cause to arrest does not automatically provide probable cause to search the arrestee's home."); *United States v. Santarsiero*, 566 F. Supp. 536, 538 (S.D.N.Y. 1983) ("Probable cause to arrest an individual does not, in and of itself, provide probable cause to search that person's home or car."). Rather, the probable cause must be based on "a sufficient nexus between the criminal activities alleged" and the location or items searched. *United States v. Singh*, 390 F.3d 168, 182 (2d Cir. 2004). In particular, searches must be supported by probable cause showing that there is a "fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. 213, 238, 103 S. Ct. 2317, 2332 (1983).

Here, the Government did not provide a sound basis to conclude that Defendants' cell phones would contain evidence of wrongdoing. The only nexus identified between Mr. Code's phone and his alleged criminality is that he used the phone for thirteen calls.[2] However, the

[2] As detailed above, one call merely referenced a text message.

content of those calls does not reside on Mr. Code's phone. The assertion that Mr. Code may be engaged in alleged criminal activity as a general matter does not give the government license to rummage through the data stored on his phone. *See, e.g.*, *United States v. Moran*, 349 F. Supp. 2d 425, 476 (N.D.N.Y. 2005) (evidence of multiple calls between defendant and a drug trafficking co-conspirator is an "insufficient basis for finding probable cause to search [defendant's] residence.").

The same is equally true for Mr. Dawkins. With the exception of a single intercepted text message, the Dawkins Applications fails to set forth any nexus between his alleged misconduct and the data stored on his phone. Nor can probable cause be found in the FBI agent's bare assertion that cell phones that have been used to communicate with others about fraud schemes "[redacted]." (Ex. 1 at MC_00000016, ¶21.); *see, e.g, United States v. Rutherford*, 71 F. Supp. 3d 386, 392 (S.D.N.Y. 2014) ("a conclusory legal allegation is insufficient to establish the existence of probable cause sufficient to support the issuance of a search warrant."); *United States v. Kortright*, No. 10 Cr. 937(KMW), 2011 WL 4406352, at *7 (S.D.N.Y. Sept. 13, 2011) (finding no probable cause to search defendant's residence based on the agent's opinion that it is common for drug traffickers to store contraband at their residence); *United States v. Guzman*, No. S5 97 CR 786(SAS), 1998 WL 61850, at *4 (S.D.N.Y. Feb. 13, 1998) ("Permitting 'a search warrant based solely on the self-avowed expertise of a law-enforcement agent, without any other factual nexus to the subject property, would be an open invitation to vague warrants authorizing virtually automatic searches of any property used by a criminal suspect.'") (quoting

United States v. Rosario, 918 F. Supp. 524, 531 (D.R.I. 1996)).

Permitting a search of all of the data stored on Defendants' cell phones based on the fact that they used them to make phone calls is no different than permitting the Government to search the photo albums and videotapes found in a person's home simply because that person made phone calls from his landline. In fact, searching an individual's cell phone is an even ***greater*** invasion of his privacy than is searching his home. As the Supreme Court explained, "a cell phone search would typically expose to the government far ***more*** than the most exhaustive search of a house: A phone not only contains in digital form many sensitive records previously found in the home; it also contains a broad array of private information never found in a home in any form—unless the phone is." *Riley*, 134 S. Ct. at 2491 (emphasis added).

Because the facts set forth in the Warrant Applications do not establish probable cause to seize and search Defendants' cell phones, evidence obtained as a result of these searches should be suppressed.

B. The Warrants are Overbroad Because They do not Limit the Scope of the Searches to the Locations of Data for Which There Exists Probable Cause to Search.

Evidence from Defendants' cell phones must also be suppressed because the Search Warrants were overbroad. Based on evidence that the phones were used for some number of calls, one of which referenced a text message,[3] and in the case of Mr. Dawkins, a single text message, the Warrants permitted a search of all the electronic data on the phones. The Warrants in no way limited the scope of the authorized search to the locations of electronic data on the phone for which there would be probable cause to believe evidence of a crime may be found. *Garrison*, 480 U.S. at 84, 107 S. Ct. at 1016 ("By limiting the authorization to search to the specific areas

[3] According to the Code Application, Mr. Dawkins said he would send a text message to Mr. Code. (Ex. 1 at MC_00000014, ¶17(b).)

and things for which there is probable cause to search, the [Fourth Amendment] ensures that the search will be carefully tailored to its justifications, and will not take on the character of the wide-ranging exploratory searches the Framers intended to prohibit.").

The Warrants authorized "[redacted]." (Ex. 3 at MC_00000115; Ex. 4 at CD_00000184) (emphasis added). In performing this examination, law enforcement was authorized to "[redacted]" (*Id.* (emphasis added).)

The allegations in the Warrant Applications do not support the all-encompassing sweep of electronically stored information that the Warrants authorized. *See United States v. Juarez*, No. 12 CR 59 (RRM), 2013 WL 357570, at *3 (E.D.N.Y. Jan. 29, 2013) (Second Circuit precedent "guards against a general search of all of [a cell phone's] records, files and data."); *United States v. Vilar*, No. S305 Cr. 621, 2007 WL 1075041, at *20 (S.D.N.Y. Apr. 4, 2007) (probable cause to search certain offices for certain documents did not support the broad seizure of ***all*** business records).

Several decisions are particularly instructive here. In *United States v. Winn,* 79 F. Supp. 3d 904, 909 (S.D. Ill. 2015), which District Judge Alison J. Nathan recently cited with approval, the defendant was alleged to have used his cell phone to photograph or videotape a group of teenage girls in their swimsuits without permission. 79 F. Supp. 3d 904, 909 (S.D. Ill. 2015); *see Wey*, 256 F. Supp. 3d at 392 (citing *Winn*). Law enforcement confiscated the defendant's phone and applied for a warrant to search it nine days later. *Winn*, 79 F. Supp. 3d at 910-11. The application, which was approved by the reviewing Judge, listed a number of items to be seized

from the phone, including "any or all files contained on said cell phone and its SIM Card or SD Card[.]" *Id*. at 911. The defendant moved to suppress the evidence obtained from his cell phone, arguing that the search warrant was impermissibly overbroad. *Id*. at 912. The district court agreed, noting that although there was probable cause to believe that ***photos*** and ***videos*** on the defendant's phone would contain evidence of public indecency, nothing in the search warrant application offered any basis to believe that the calendar, phonebook, contacts, SMS messages, MMS messages, emails, ringtones, audio files, call logs, installed application data, GPS information, WIFI information, internet history and usage, or system files were connected with the defendant's alleged crime. *Id*. at 919-20. As the court explained, the warrant application:

> establishe[d] that the police had probable cause to look for and seize a very small and specific subset of data on [the defendant's] cell phone. ***But the warrant did not limit the scope of the seizure to only that data or describe that data with as much particularity as the circumstances allowed. Instead, the warrant contained an unabridged template that authorized the police to seize the entirety of the phone and rummage through every conceivable bit of data***, regardless of whether it bore any relevance whatsoever to the criminal activity at issue. Simply put, the warrant told the police to take everything, and they did. As such, the warrant was overbroad in every respect and violated the Fourth Amendment.

Id. at 922 (emphasis added); *see also Wey*, 256 F. Supp. 3d at 392 (quoting *Winn* for the proposition that "if [the applying officer] wants to seize every type of data from the cell phone, then it was incumbent upon him to explain in the complaint how and why each type of data was connected to [Defendant's] criminal activity, and he did not do so.") (quotation marks omitted). As a result, the court suppressed all evidence seized pursuant to the search warrant. *Winn*, 79 F. Supp. 3d at 926-27 (explaining that the warrant was a general warrant because "[e]very portion is impossibly overbroad, encompassing every conceivable bit of data generated by the use of the cell phone at any point in time" and that "'the only remedy for a general warrant is to suppress all evidence obtained thereby.'") (quoting *United States v. Yusuf*, 461 F.3d 374, 393 (3d Cir. 2006)).

Similarly, in *In re Nextel Cellular Telephone,* No. 14 MJ 8005, 2014 WL 2898262, at *1-2 (D. Kan. June 26, 2014), law enforcement submitted an application for a warrant to search the contents of a cell phone seized incident to an arrest for drug trafficking. No. 14 MJ 8005, 2014 WL 2898262, at *1-2 (D. Kan. June 26, 2014). Like the Warrants here, the application sought to conduct a "full and complete forensic telephone examination" of the cell phone.[4] *Id*. at *2. The court denied the application as patently overbroad, noting in particular that the search methodology "will result in the overseizure of data and indefinite storage of data that it lacks probable cause to seize" and that it was "so broad that it appears to be nothing more than a 'general, exploratory rummaging in a person's belongings.'" *Id*. at *10 (*quoting Coolidge* 403 U.S. at 467). "Put another way", the court explained, "'[j]ust as probable cause to believe that a stolen lawnmower may be found in a garage will not support a warrant to search an upstairs bedroom,' probable cause to believe drug trafficking communication may be found in [a] phone's [] mail application will not support the search of the phone's Angry Birds application." *Id*. at *13 (*quoting United States v. Ross*, 456 U.S. 798, 824 (1982)).

The Warrants in this case fare no better. To the extent that this Court concludes that the Warrants established probable cause to seize and search Defendants' phones in any manner, the search of those phones should have been limited to the locations on the phones where, according to the Applications, there was probable cause to conclude evidence of criminality would be found. Even assuming—the Code Application asserts—that cell phones used to communicate with others about fraud schemes "often contain records of that activity," those "records" here

[4] The search methodology at issue in *Nextel* included: "searching for and attempting to recover any deleted, hidden, or encrypted data . . . surveying various file directories and the individual files they contain; opening files in order to determine their contents; scanning storage areas; [and] performing keyword searches through all electronic storage areas[.]" *Id*.

would be, at best, records of phone calls and a single text message. The Warrants, however, contained no limitation on the scope of the authorized searches. As in *Winn*, the Warrants authorized the Government to conduct "[redacted]" (*See* Ex. 3 at MC_00000115; Ex. 4 at CD_00000184) (emphasis added). Furthermore, the search methodology permitted by the Warrants is indistinguishable from the methodology that the court rejected as patently overbroad in *Nextel*, allowing law enforcement personnel to rummage through the entirety of the data contained on Defendants' phones to fish for evidence.

The Warrants contained no limitation whatsoever on the categories of data on Defendants' phones that the Government could search. Instead, the Warrants essentially "told the police to take everything, and they did." *Winn*, 79 F. Supp. 3d at 922. Because the Search Warrants permitted the Government to "rummage through every conceivable bit of data" contained on Defendants' cell phones, *Winn*, 79 F. Supp. 3d at 922, they were, "in function if not in form," general warrants. *Wey*, 256 F. Supp. 3d at 386. The Warrants were thus overbroad and violated the Fourth Amendment.

C. All Evidence Derived From the Unlawful Search of Defendants' Cell Phones Should be Suppressed.

The Fourth Amendment's exclusionary rule "forbids the use of improperly obtained evidence at trial." *Herring v. United States*, 555 U.S. 135, 139 (2009). Although the exclusionary rule contains a good faith exception, "[g]ood faith is not a magic lamp for police officers to rub whenever they find themselves in trouble." *United States v. Reilly*, 76 F.3d 1271, 1280 (2d Cir. 1996). Regardless of an officer's good faith, the Fourth Amendment requires suppression where an invalidated warrant is based upon an "affidavit so lacking in indicia of probable cause as to

render official belief in its existence entirely unreasonable." *United States v. Leon*, 468 U.S. 897, 923 (1984) (internal citation and quotation marks omitted). Moreover, as detailed above, the government bears the burden "'to demonstrate the objective reasonableness of the officers' good faith reliance' on an invalidated warrant." *United States v. Clark*, 638 F.3d 89, 100 (2d Cir. 2011) (quoting *United States v. George*, 975 F.2d 72, 77 (2d Cir. 1992)).

Here, because the Government lacked probable cause to search the entirety of the data contained on Defendants' cell phones, the Warrants were patently overbroad, and any law enforcement officer's reliance upon them was unreasonable. *See Leon*, 468 U.S. at 923. Indeed, the Warrants were so patently overbroad that the good faith exception to the exclusionary rule cannot apply. *See, e.g.*, *Wey*, 256 F. Supp. 3d at 410–411 (suppressing all evidence obtained from overbroad warrant); *Winn*, 79 F. Supp. 3d 926–27 (same). Accordingly, all evidence seized pursuant to the unconstitutional Warrants, as well as all evidence derived from such evidence, should be suppressed.[5] *See, e.g.*, *United States v. Bershchansky*, 788 F.3d 102, 112 (2d Cir. 2015) ("Exclusion extends to both physical evidence and indirect products of unlawful searches . . . .").

CONCLUSION

Accordingly, this Court should suppress the evidence obtained from the searches of Defendants' cell phones and order the Government to immediately return Defendants' cell phones, as well as the imaged copies of the cell phone data it maintains, to Defendants.

[5] Messrs. Code and Dawkins have standing to move for suppression because they maintain a reasonable expectation of privacy in their cell phones. *See Mancusi v. DeForte*, 392 U.S. 364, 369, 88 S. Ct. 2120, 2124 (1968); *see also United States v. Herron*, 2 F. Supp. 3d 391, 401 (E.D.N.Y. 2014) (defendant had a reasonable expectation of privacy in a cell phone because he was its "sole user"); Ex. 5 (Code Affidavit); Ex. 6 (Dawkins Affidavit).

Dated: New York, New York
December 3, 2018

Respectfully submitted,

NEXSEN PRUET LLC

By: /s/ Mark. C. Moore
William W. Wilkins
Mark C. Moore
Andrew A. Mathias
55 E. Camperdown Way, Suite 400
Greenville, South Carolina 29601
(864) 370-2211
Attorneys for Defendant Merl Code

HANEY LAW GROUP PLLC

By: /s/ Steven A. Haney
Steven A. Haney
3000 Town Center Drive, Suite 2570
Southfield, Michigan 48075
(248) 414-1470
Attorneys for Defendant Christian Dawkins

BARNES AND THORNBURG, LLP

By: /s/ William R. Martin
William R. Martin
1717 Pennsylvania Ave
Suite 500
Washington, DC 20006
(202) 465-8422
Attorneys for Defendant Lamont Evans

LAW OFFICES OF JEFFREY LICHTMAN

By: /s/ Jeffrey B. Einhorn
Jeffrey B. Einhorn
Jeffrey Lichtman
11 E. 44th Street, Ste. 501
New York, New York 10017
(212) 581-1001
Attorneys for Defendant Anthony "Tony" Bland

MORDOCK BARBER, LLC

By: /s/ Craig J. Mordock
Craig J. Mordock
7611 Maple Street, Suite A3
New Orleans, Louisiana 70118
(504) 304-2335
Attorneys for Defendant Emanuel "Book" Richardson